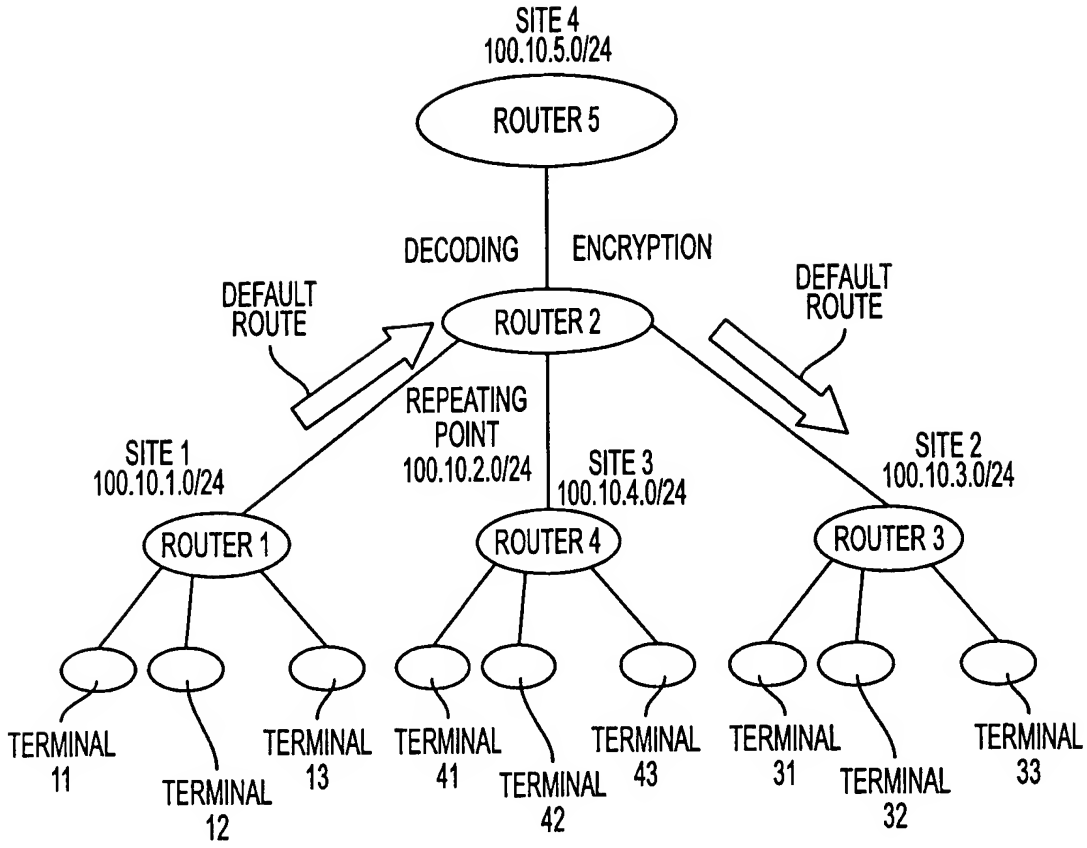
SITE 4
100.10.5.0/24
ROUTER 5
DECODING
ENCRYPTION
DEFAULT
ROUTE
ROUTER 2
DEFAULT
ROUTE
REPEATING
POINT
100.10.2.0/24
SITE 1
100.10.1.0/24
SITE 3
100.10.4.0/24
SITE 2
100.10.3.0/24
ROUTER 1
ROUTER 4
ROUTER 3
TERMINAL
11
TERMINAL
12
TERMINAL
13
TERMINAL
41
TERMINAL
42
TERMINAL
43
TERMINAL
31
TERMINAL
32
TERMINAL
33

FIG. 1

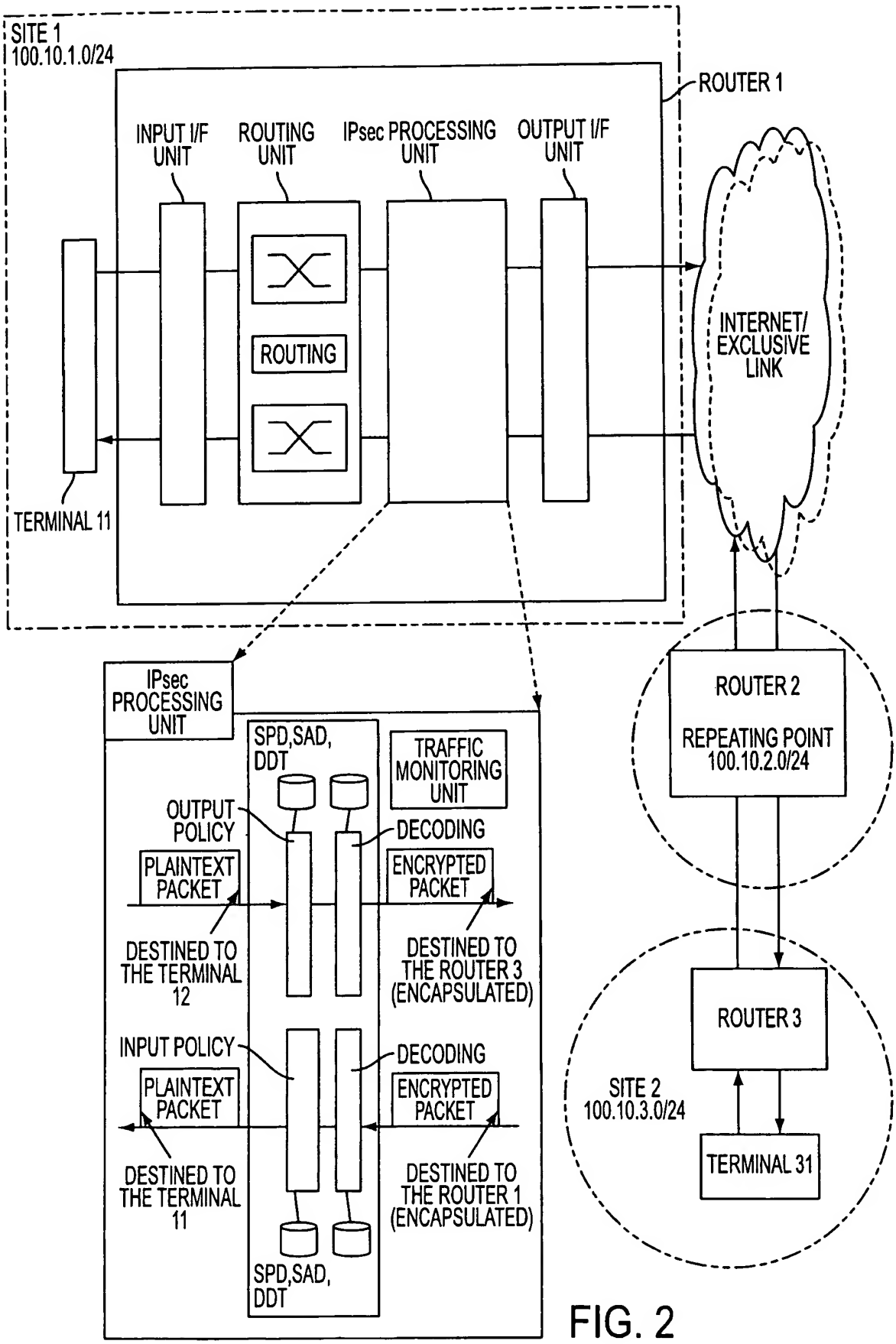
SITE 1
100.10.1.0/24
ROUTER 1
INPUT I/F UNIT
ROUTING UNIT
IPsec PROCESSING UNIT
OUTPUT I/F UNIT
ROUTING
INTERNET/ EXCLUSIVE LINK
TERMINAL 11
IPsec PROCESSING UNIT
SPD,SAD, DDT
TRAFFIC MONITORING UNIT
OUTPUT POLICY
DECODING
PLAINTEXT PACKET
ENCRYPTED PACKET
DESTINED TO THE TERMINAL 12
DESTINED TO THE ROUTER 3 (ENCAPSULATED)
INPUT POLICY
DECODING
PLAINTEXT PACKET
ENCRYPTED PACKET
DESTINED TO THE TERMINAL 11
DESTINED TO THE ROUTER 1 (ENCAPSULATED)
SPD,SAD, DDT
ROUTER 2
REPEATING POINT
100.10.2.0/24
ROUTER 3
SITE 2
100.10.3.0/24
TERMINAL 31

FIG. 2

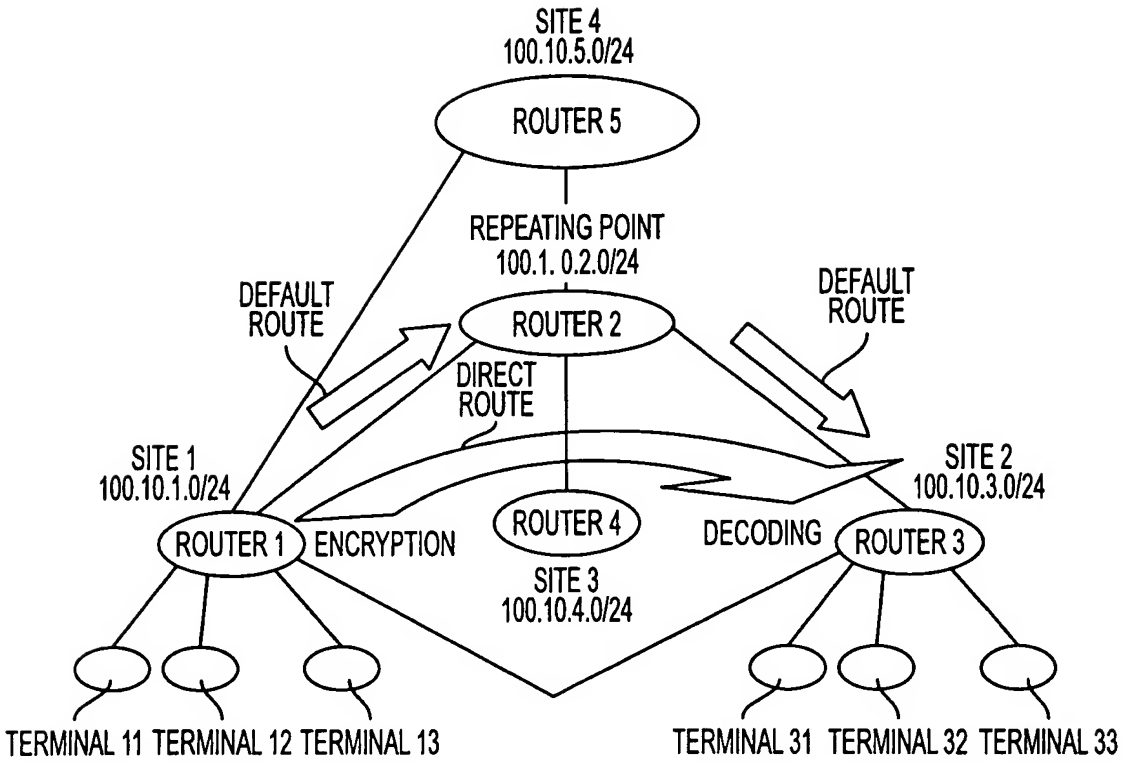
SITE 4
100.10.5.0/24
ROUTER 5
REPEATING POINT
100.1. 0.2.0/24
DEFAULT
ROUTE
ROUTER 2
DEFAULT
ROUTE
DIRECT
ROUTE
SITE 1
100.10.1.0/24
SITE 2
100.10.3.0/24
ROUTER 1
ENCRYPTION
ROUTER 4
SITE 3
100.10.4.0/24
DECODING
ROUTER 3
TERMINAL 11
TERMINAL 12
TERMINAL 13
TERMINAL 31
TERMINAL 32
TERMINAL 33

FIG. 3

SPD (SECURITY POLICY DATABASE)

START POINT IP ADDRESS	END POINT IP ADDRESS	LINK NO.	POLICY	PROTOCOL	DIRECT FLAG
100.10.1.0/24	100.10.3.0/24	1	ENCRYPTION	ANY	DEFAULT
100.10.1.0/24	100.10.3.0/24	2	ENCRYPTION	ANY	DIRECT
100.10.1.0/24	100.10.5.0/24	3	NON-ENCRYPTION		
100.10.1.0/24	100.10.6.0/24		DESTRUCTION		

FIG. 4

DDT (DEFAULT/DIRECT TABLE)

DESTINATION IP ADDRESS	TRANSFER DESTINATION IP ADDRESS	POLICY	IDENTIFICATION FLAG	DRIVE REQUEST	.....
100.10.3.0/24	100.10.3.0/24	ENCRYPTION	DEFAULT		
100.10.4.0/24	100.10.4.0/24	ENCRYPTION	DIRECT	OFF	

FIG. 5

SAD (SECURITY ASSOCIATION DATABASE)

END POINT IP ADDRESS OF EXTERNAL HEADER	LINK NO.	CLASS OF IPsec PROTOCOL	SPI VALUE	OTHER SA PARAMETER	DIRECT INDICATION
100.10.2.1	1	ESP	0x32e9a7c6	....	DEFAULT
100.10.3.1	2	ESP	0x32e9a7c8	....	DIRECT
100.10.5.1	3				
100.10.6.1					

SPI: SECURITY PARAMETER INDEX
ESP: ENCAPSULATING SECURITY PAYLOAD

FIG. 6

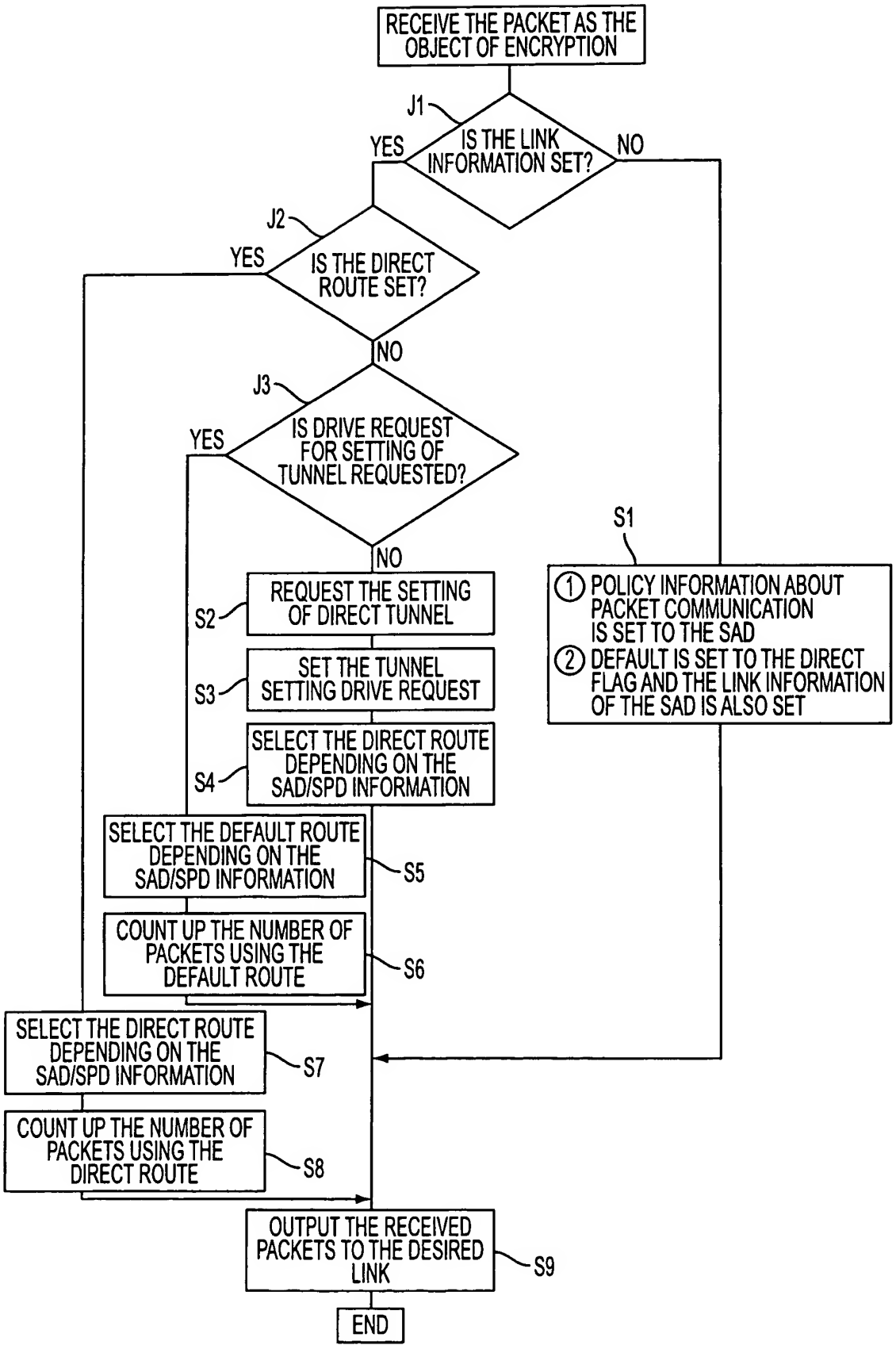
RECEIVE THE PACKET AS THE OBJECT OF ENCRYPTION
J1
IS THE LINK INFORMATION SET?
YES
NO
J2
IS THE DIRECT ROUTE SET?
YES
NO
J3
IS DRIVE REQUEST FOR SETTING OF TUNNEL REQUESTED?
YES
NO
S1
① POLICY INFORMATION ABOUT PACKET COMMUNICATION IS SET TO THE SAD
② DEFAULT IS SET TO THE DIRECT FLAG AND THE LINK INFORMATION OF THE SAD IS ALSO SET
S2
REQUEST THE SETTING OF DIRECT TUNNEL
S3
SET THE TUNNEL SETTING DRIVE REQUEST
S4
SELECT THE DIRECT ROUTE DEPENDING ON THE SAD/SPD INFORMATION
SELECT THE DEFAULT ROUTE DEPENDING ON THE SAD/SPD INFORMATION
S5
COUNT UP THE NUMBER OF PACKETS USING THE DEFAULT ROUTE
S6
SELECT THE DIRECT ROUTE DEPENDING ON THE SAD/SPD INFORMATION
S7
COUNT UP THE NUMBER OF PACKETS USING THE DIRECT ROUTE
S8
OUTPUT THE RECEIVED PACKETS TO THE DESIRED LINK
S9
END

FIG. 7

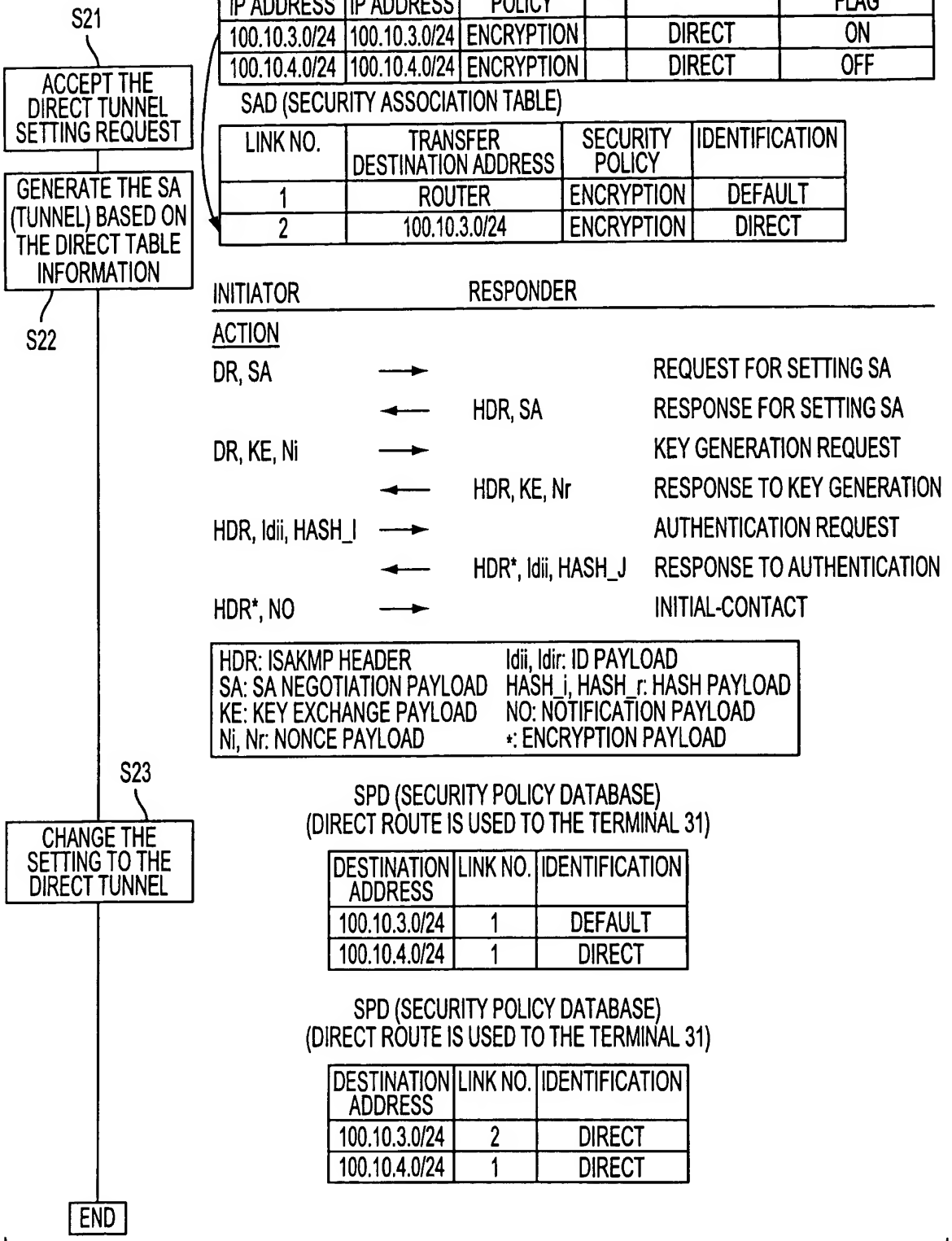
S21
ACCEPT THE DIRECT TUNNEL SETTING REQUEST
GENERATE THE SA (TUNNEL) BASED ON THE DIRECT TABLE INFORMATION
S22
S23
CHANGE THE SETTING TO THE DIRECT TUNNEL
END
DDT (DEFAULT/DIRECT TABLE)
START POINT IP ADDRESS | END POINT IP ADDRESS | SECURITY POLICY | ... | IDENTIFICATION | DRIVE REQUEST FLAG
100.10.3.0/24 | 100.10.3.0/24 | ENCRYPTION | | DIRECT | ON
100.10.4.0/24 | 100.10.4.0/24 | ENCRYPTION | | DIRECT | OFF
SAD (SECURITY ASSOCIATION TABLE)
LINK NO. | TRANSFER DESTINATION ADDRESS | SECURITY POLICY | IDENTIFICATION
1 | ROUTER | ENCRYPTION | DEFAULT
2 | 100.10.3.0/24 | ENCRYPTION | DIRECT
INITIATOR RESPONDER
ACTION
DR, SA → REQUEST FOR SETTING SA
← HDR, SA RESPONSE FOR SETTING SA
DR, KE, Ni → KEY GENERATION REQUEST
← HDR, KE, Nr RESPONSE TO KEY GENERATION
HDR, Idii, HASH_I → AUTHENTICATION REQUEST
← HDR*, Idii, HASH_J RESPONSE TO AUTHENTICATION
HDR*, NO → INITIAL-CONTACT
HDR: ISAKMP HEADER
SA: SA NEGOTIATION PAYLOAD
KE: KEY EXCHANGE PAYLOAD
Ni, Nr: NONCE PAYLOAD
Idii, Idir: ID PAYLOAD
HASH_i, HASH_r: HASH PAYLOAD
NO: NOTIFICATION PAYLOAD
*: ENCRYPTION PAYLOAD
SPD (SECURITY POLICY DATABASE)
(DIRECT ROUTE IS USED TO THE TERMINAL 31)
DESTINATION ADDRESS | LINK NO. | IDENTIFICATION
100.10.3.0/24 | 1 | DEFAULT
100.10.4.0/24 | 1 | DIRECT
SPD (SECURITY POLICY DATABASE)
(DIRECT ROUTE IS USED TO THE TERMINAL 31)
DESTINATION ADDRESS | LINK NO. | IDENTIFICATION
100.10.3.0/24 | 2 | DIRECT
100.10.4.0/24 | 1 | DIRECT

FIG. 8

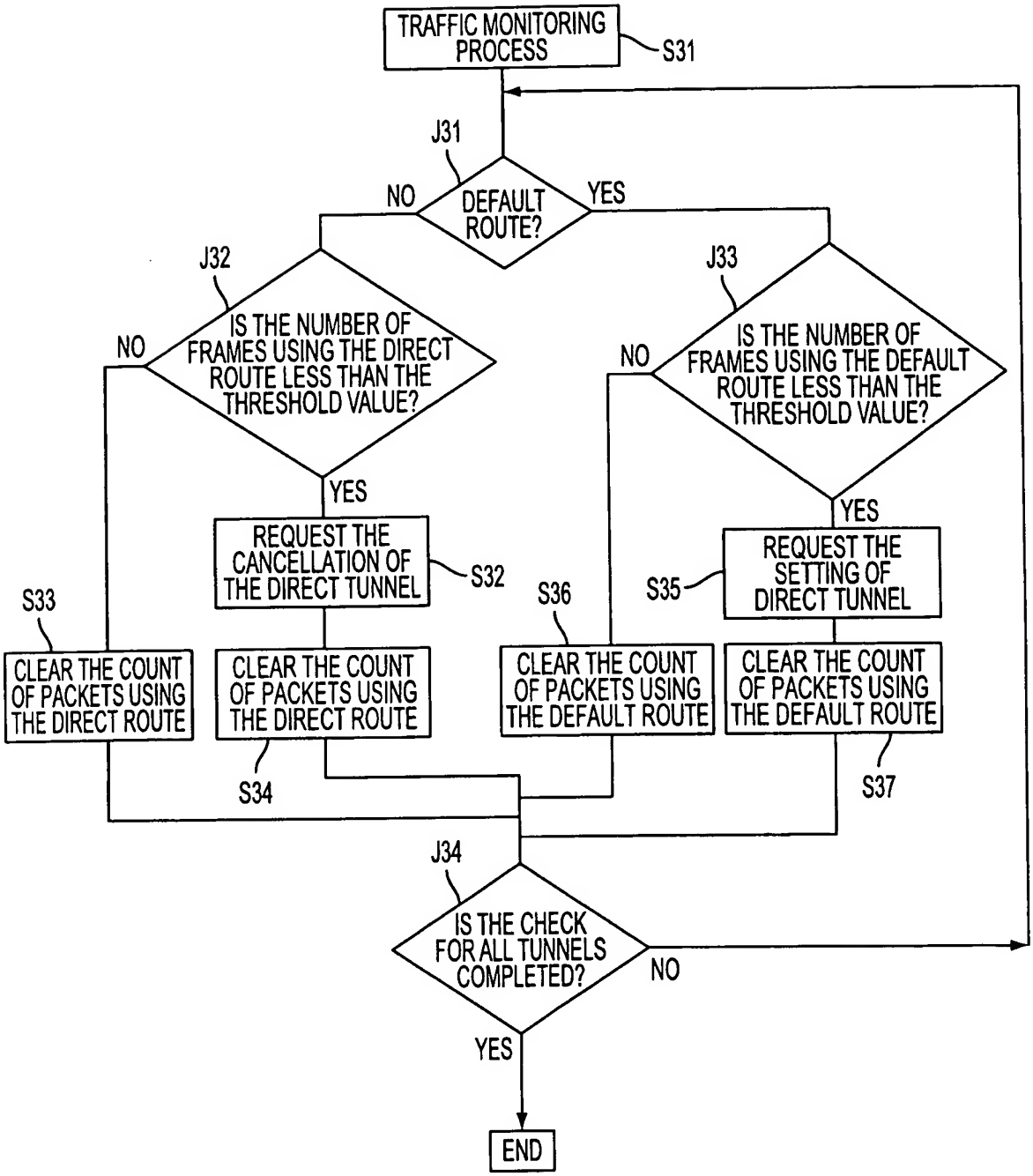
TRAFFIC MONITORING PROCESS
S31
J31
DEFAULT ROUTE?
NO
YES
J32
IS THE NUMBER OF FRAMES USING THE DIRECT ROUTE LESS THAN THE THRESHOLD VALUE?
NO
YES
J33
IS THE NUMBER OF FRAMES USING THE DEFAULT ROUTE LESS THAN THE THRESHOLD VALUE?
NO
YES
REQUEST THE CANCELLATION OF THE DIRECT TUNNEL
S32
REQUEST THE SETTING OF DIRECT TUNNEL
S35
S33
CLEAR THE COUNT OF PACKETS USING THE DIRECT ROUTE
CLEAR THE COUNT OF PACKETS USING THE DIRECT ROUTE
S34
S36
CLEAR THE COUNT OF PACKETS USING THE DEFAULT ROUTE
CLEAR THE COUNT OF PACKETS USING THE DEFAULT ROUTE
S37
J34
IS THE CHECK FOR ALL TUNNELS COMPLETED?
NO
YES
END

FIG. 9

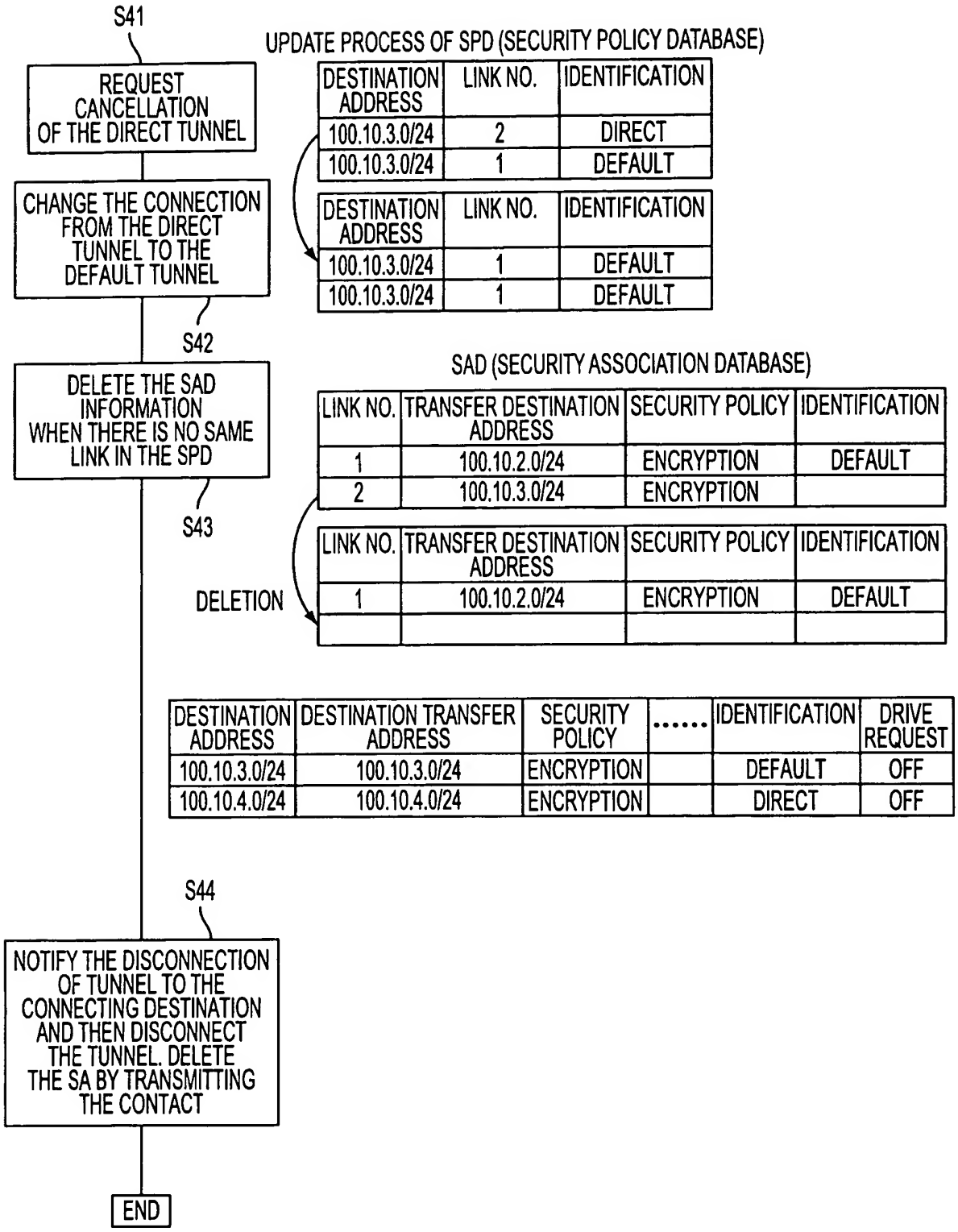
S41
REQUEST CANCELLATION OF THE DIRECT TUNNEL
CHANGE THE CONNECTION FROM THE DIRECT TUNNEL TO THE DEFAULT TUNNEL
S42
DELETE THE SAD INFORMATION WHEN THERE IS NO SAME LINK IN THE SPD
S43
S44
NOTIFY THE DISCONNECTION OF TUNNEL TO THE CONNECTING DESTINATION AND THEN DISCONNECT THE TUNNEL. DELETE THE SA BY TRANSMITTING THE CONTACT
END
UPDATE PROCESS OF SPD (SECURITY POLICY DATABASE)
DESTINATION ADDRESS | LINK NO. | IDENTIFICATION
100.10.3.0/24 | 2 | DIRECT
100.10.3.0/24 | 1 | DEFAULT
DESTINATION ADDRESS | LINK NO. | IDENTIFICATION
100.10.3.0/24 | 1 | DEFAULT
100.10.3.0/24 | 1 | DEFAULT
SAD (SECURITY ASSOCIATION DATABASE)
LINK NO. | TRANSFER DESTINATION ADDRESS | SECURITY POLICY | IDENTIFICATION
1 | 100.10.2.0/24 | ENCRYPTION | DEFAULT
2 | 100.10.3.0/24 | ENCRYPTION
DELETION
LINK NO. | TRANSFER DESTINATION ADDRESS | SECURITY POLICY | IDENTIFICATION
1 | 100.10.2.0/24 | ENCRYPTION | DEFAULT
DESTINATION ADDRESS | DESTINATION TRANSFER ADDRESS | SECURITY POLICY | ..... | IDENTIFICATION | DRIVE REQUEST
100.10.3.0/24 | 100.10.3.0/24 | ENCRYPTION | | DEFAULT | OFF
100.10.4.0/24 | 100.10.4.0/24 | ENCRYPTION | | DIRECT | OFF

FIG. 10